

BIC
CONF

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

B2
J'

9. (Twice Amended) A method for providing updated encryption key pairs in a public key system comprising the steps of:

providing, through a multi-client manager unit, selectable expiry data including public encryption key expiry data associated with a public encryption key, [and selectable private key expiry data] that is selectable on a per client basis;

digitally storing selected public encryption key expiry data for association with a new encryption key pair; [and]

generating a new encryption key pair that is not computable from a previous encryption key pair; and

associating the stored selected expiry data with the new encryption key pair to affect a transition from an old encryption key pair to a new encryption key pair.

Sub
B3

14. (Twice Amended) A system for providing updated digital signature key pairs in a public key system comprising:

multi-client manager means for providing selectable digital signature expiry data including at least both public verification key expiry data and selectable private signing key expiry data that is selectable on a per client basis wherein the digital signature key pairs are not shared among users;

means, accessible by the multi-client manager means, for digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

means, responsive to the stored selected public key expiry data, for associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

Sub 3
B4

21. (Twice Amended) A storage medium comprising:

- a stored program for execution by a processor wherein the program facilitates providing updated digital signature key pairs in a public key system by:
 - allowing entry of selectable expiry data including both at least public verification key expiry data and selectable signing private key expiry data that [is] are selectable on a per client basis wherein the digital signature key pairs are not shared among users;
 - digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and
 - associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

B5

24. (Twice Amended) The storage medium of claim 21 wherein the stored program further facilitates

- determining whether a digital signature key pair update request has been received from a client unit;
- receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request; and
- creating a new digital signature certificate containing the selected public key expiry data selected for the client that generated the digital signature key pair update request.

In claim 26, line 1, please delete "claim 19" and insert therefor --claim 21--.

Response

The application has been finally rejected. Applicants respectfully traverse and request reconsideration.

Applicants will submit a supplemental declaration upon notice of allowable claims.